NAIC-ID(RS)T-0267-95

NATIONAL AIR INTELLIGENCE CENTER

ANALYSIS OF THE REALITY AND FEASIBILITY OF COMPUTER COUNTERMEASURES

by

Jang Ji

NAIC- ID(RS)T-0267-95

HUMAN TRANSLATION

NAIC-ID(RS)T-0267-95 6 November 1995

MICROFICHE NR: 95C000693

ANALYSIS OF THE REALITY AND FEASIBILITY OF COMPUTER COUNTERMEASURES

English pages: 17

Source: Ji Suan Ji Dui Kang De Xian Shi Xing He Ke Xing Xing Fen Xi; pp. 54-60

Country of origin: China
Translated by: SCITRAN
F33657-84-D-0096
Requester: NAIC/TASC/John L. Gass
Approved for public release: distribution unlimited.

THIS TRANSLATION IS A RENDITION OF THE ORIGINAL FOREIGN TEXT WITHOUT ANY ANALYTICAL OR EDITORIAL COMMENT STATEMENTS OR THEORIES ADVOCATED OR IMPLIED ARE THOSE OF THE SOURCE AND DO NOT NECESSARILY REFLECT THE POSITION OR OPINION OF THE NATIONAL AIR INTELLIGENCE CENTER.	PREPARED BY: TRANSLATION SERVICES NATIONAL AIR INTELLIGENCE CENTER WPAFB, OHIO

NAIC- ID(RS)T-0267-95 Date 6 November 1995

ABSTRACT Systematic presentation of the concepts and contents of relevent computer countermeasures. Qualitative analysis of the reality and feasibility of computer countermeasures. In conjunction with this, presents several concrete suggestions to develop computer countermeasures.

KEY TERMS Electronic countermeasures Computer Computer--electronic countermeasures

GRAPHICS DISCLAIMER

All figures, graphics, tables, equations, etc. merged into this translation were extracted from the best quality copy available.

1 INTRODUCTION

Following along with the rapid development of microelectronic technology, the level of reliance of opposing sides on computers will get higher and higher. Computers are the key equipment raising modern "hard damage" weapons system control capabilities and killing and damaging power. They are also the "nerve centers" of modern military forces--the core of C3I systems. The more modernized the equipment of modern military forces is, the greater the reliance on computers then is. Once computer systems in modernized military forces receive "jamming, destruction, and damage", the consequences are unthinkable.

As far as the advent and spread of computer viruses are concerned, they pose a new challenge to the safety and protection, development, and application of computers. They also make computer virus countermeasures (CVCM) into an effective means of attacking enemy computer equipment, systems, or networks. As a matter of fact, since the early period of the application of computers to the military realm, computer countermeasures penetrated into the realm of military countermeasures. The appearance of computer virus countermeasure (CVCM) means has pushed forward a new electronic countermeasures realm--the formation and development of computer opposition.

Computer opposition refers to the use of various types of means and measures including within them comprehensive opposition actions such as computer virus countermeasure (CVCM) means, carrying out attacks on enemy computer equipment, systems, and networks, or stealing intelligence relating to them, or disrupting, destroying, and smashing their combat effectiveness, and, in conjunction with this, avoiding or lowering enemy attacks suffered by our side's computer equipment, systems, and networks. It is the newest realm in modern electronic countermeasures, and will also become the principal part of C3I countermeasures (C3ICM).

2 THE CONTENT OF COMPUTER COUNTERMEASURES

The content of computer countermeasures primarily include computer countermeasure reconnaissance, jamming, destruction, as well as such contents as computer countermeasure counterreconnaissance, counterjamming, and counterdestruction.

(1) Computer Countermeasure Recconnaisance

Making use of specialized equipment (computer counter reconnaissance systems), military actions associated with stealing information in enemy computer systems, ascertaining the system structural characteristics and properties, as well as factors advantageous to the implementation of defensive computer countermeasures as well as the implementation of computer countermeasure jamming, detecting computer countermeasure reconnaissance and jamming threats coming from the enemy side.

(2) Computer Countemeasure Jamming

Integrated attack actions making use of computer countermeasure jamming equipment to carry out destruction, disruption, and deception against enemy computer equipment, systems, or networks. Depending on the target catagory of attack, it is possible to separate them into environmental jamming, hardware jamming, and software jamming.

a. Environmental Jamming

Computer countermeasure jamming carried out with the purpose of destroying normal enemy computer operations aiming at weaknesses associated with computer dependence on special environments. This can be divided into electromagnetic field jamming, static electric jamming, electric power source jamming, and so on.

Electromagnetic field jamming is the use of electronic jamming means to make enemy computer equipment be placed in sustained high peak value field strength environments or conditions to reach the objective of disrupting their operations. Data clearly shows that, "Computers in 1V/m electric field strengths are capable of operating normally. Exceeding 5V/m will then show the appearance of program errors. Small signal circuits--for example, magnetic discs, magnetic tape, and so on--permit erroneous outputs in 5V/m electric field strengths. As far as memory storage devices in 15V/m and data transform devices in 50V/m are concerned, there is not way for them to operate normally in both cases." Magnetic recording equipment used by computer systems--for example, magnetic discs, magnetic tape, and so on--are also very sensitive to peripheral magnetic field strengths. "If one makes use of 1.1x105 A/m magnets to interfer (placed in the vicinity of magnetic tape spools with plastic protective rings) with magnetic tape spools, then, there will be one third of a 732m long magnetic tape that will lose information".

Static electricity jamming is electronic jamming which--at the same time as destroying magnetic recording--creates static electricity discharges associated with computer equipment or carrier platforms in order to disrupt computer system operations. It already constitutes a severe threat to modern computer systems widely employing CMOS components. Oxydation layers of MOS components are normally thermally generated SiO2 . The critical electric field strength is 5-8V/m. MOS component grid electrode thickness is 0.15 microns. Theoretical breakdown voltages can reach 75-120V. However, in reality, breakdown voltages are very low, causing MOS components, for very small amounts of electricity, to still induce relatively large static electricity voltages, leading to MOS component grid breakdown.

Electric power source jamming is making use of electric power source lead lines to bring in power source voltages or currents of a shocking nature, leading to the generation of confusion in digital or pulse data associated with computer systems. Electrical power source jamming is jamming phenomena which exist universally in electronic systems. With regard to computer systems which opt for the use of digital circuitry, it is even more effective. As far as transient voltage and current shocks given rise to by electrical power source voltage fluctuations or sudden changes of large amplitude in loads associated with networks are concerned, it is possible, through electric power supply lines to introduce them into computer systems and normal signal superpositions, leading to data errors.

b. Hardware Jamming

Making use of this characteristic of computer dependent digital systems has the intention of jamming hardware circuits inside computer systems, causing them to be unable to operate normally. In digital systems, due to logic components employed all having their own threshold levels and noise tolerance limits corresponding to them, if noise or pulse data intrude into computer systems, after exceeding limits which digital systems can permit, digital systems will produce erroneous operations. That is, programs can be destroyed or such things as main address lines can be jammed, leading to loss of program control. Hardware jamming can normally be divided into two large types--

nulcear electromagnetic pulse (NEMP) jamming and nonnuclear electromagnetic pulse jamming.

Nuclear electromagnetic pulse jamming is nothing else than making use of a type of transient electromagnetic radiation pulse produced during nuclear explosions to attack computer equipment and jam systems. Voltages and currents induced by high energy nuclear electromagnetic pulses will create for computer hardware--in particular, data information associated with computer memory storage--disastrous destruction. Nuclear electromagnetic pulses are capable--within a trillionth of a second--of attaining strong electric fields on the order to 104 - 105 V/m. Sustainment periods are on the order of microseconds. Transient powers reach heights of a few megwatts. Pulse leading edges are steeper by about 1000 fold than trailing edges. When a nuclear bomb with an energy on the order of megatons explodes in a 400km air burst, the nuclear electromagnetic pulse radius can reach 3200km. The possibility of integrated circuits being damaged by electromagnetic pulses is a billion times that for vaccuum tubes. Outside China, the idea has already been put forward to develop electromagnetic pulse weapons systems which--when there is a detonation at a certain altitude--does not produce nuclear shock waves or radiation on the ground but still causes the paralysis of enemy electronic equipment (including computers).

As far as nonnuclear electromagnetic pulse jamming is concerned, it makes use of nonnuclear electromagnetic pulse technology, in limited geographical areas, to create electromagnetic pulses similar to those at times of high altitude nuclear detonations, carrying out jamming or destruction of enemy electronic equipment hardware (including computer systems). The U.S. military is just in the midst of developing this type of technology. This type of weapon--using high energy radio frequency pulses to destroy military electronic systems--is also called radio frequency weapons. As far as RF/HPM (radio frequency/high power microwave) research projects which the U.S. military is in the midst of conducting are concerned, frequency ranges can be from 100MHz to 35GHz. The pulse powers can reach heights on the order of thousands of megawatts.

c. Software Jamming

Primarily supported by computer virus jamming, it goes through attacks on enemy computer software systems in order to attain the disruption of the operations of their computer equipment, systems, and networks. Speaking in terms of theory and practice, any computer system has weak points and points that are easily attacked. No operating system can be perfect in every way. This is the fundamental condition on which software jamming relies. Computer virus jamming is capable of carrying out overload, deception, disruption, and damage jamming.

Computer virus overload jamming is nothing else than making use of computer viruses capable of carrying out overload jamming to sieze control of enemy computer systems. In conjunction with this, they reproduce themselves ceaselessly or take over the use of computer system resources (CPU, internal storage, external storage, channels, networks, and so on) to create computer system and overload, and, at key moments, cause system crash. /56

Computer virus deception jamming is taking computer virus pulse code carrying false data and inputing it into enemy computer systems and networks--in particular, enemy electronic intelligence collection, handling, and distribution systems--using active strategies to deceive enemy computer intelligence analysis and handling systems or to alter the original information data in enemy computer systems. It is also possible to intentionally alter key data and command codes in enemy command systems, control systems, and communication systems to attain the objectives of deceptive jamming.

Computer virus disruptive jamming refers to being able--after a certain period following computer viruses infecting enemy computer systems--to declare their existence, forcing the enemy to isolate the infected equipment and systems, with the intention of attaining the exhaustion and crippling of the entire enemy combat capability.

Computer virus damage jamming is using computer viruses to destroy programs and data in various types of enemy computer systems, causing the complete paralysis of the systems.

Computer virus jamming constitutes a severe threat to computer equipment, systems, and networks. They have successfully raided the U.S.'s largest and most important national defense and military computer network--the Interet. With a total of more than 6200 netted computers, it was invaded and attacked, creating network paralysis for 24 hours (netted machines reached over 25000 units). The facts clearly show that computer countermeasure jamming is the most important, highly effective, strongly offensive jamming means to date.

(3) Computer Destruction Countermeasures

They carry out strikes against enemy computer equipment, systems, and networks, or their loading platforms, making use of methods of physical destruction and damage. They are also one form of computer countermeasure. Weapons systems made use of for destruction and damage can depend on combat requirements--selecting such conventional weapons systems as artillery, aircraft, and so on. It is also possible to select laser weapons systems.

(4) Computer Countermeasure Antireconnaissance

These are combined defensive actions adopted to prevent stored information, electromagnetic information, as well as information advantageous to the enemy's carrying out computer countermeasure reconnaissance, jamming, and destruction actvities being acquired by him or to cripple enemy computer countermeasure reconnaissance effectiveness, strengthening friendly computer countermeasure results.

a. Passive Computer Countermeasure Antireconnaissance

This refers to the adopting of directed technology measures in areas, time domains, nodal points, terminals, and networks where the enemy is capable of carrying out computer countermeasure reconnaissance in order to block, cripple, and eliminate enemy detection results. Normally, the first is to avoid information security losses given rise to by system electromagnetic leaks and radiation. The second is to make use of such techniques as data classification, information security, visitor control, auit verification, and so on, to guarantee the safety and reliability of signal sources, information, and signal channels. The third is to overcome currently existing flaws in applications associated with system or network technology, to realize secure operations in whole systems.

b. Active Computer Countermeasure Antireconnaissance

This is making use of computer virus jamming means to actively attack enemy computer equipment in specialized computer countermeasure information acquistion, processing, and distribution reconnaissance systems or adopting fire power destruction methods to strike enemy computer countermeasure reconnaissance equipment to realize actions associated with secure computer system operations.

(5) Computer Countermeasure Antijamming

As far as the special characteristics and properties associated with computer countermeasure jamming carried out by the enemy against the friendly side are concerned--in particular, the characteristics during computer virus jamming--they are actions adopted to cripple and eliminate to the greatest extent possible the influences of jamming on friendly computer equipment, systems, and networks, and to guarantee normal operations. In the last two years, with respect to the more than 500 types of computer viruses which have appeared, a good number of nations and orgainizations have already developed corresponding "disinfection software". However, contradications associated with computer countermeasure jamming and antijamming are still generating new changes. All research currently in hand is only a beginning.

(6) Computer Countermeasure Antidestruction

Raising counterdestruction and damage capabilities of computer equipment, systems, and networks as well as field survivability under conditions of physical destruction and damage.

3 QUALITATIVE ANALYSIS OF COMPUTER COUNTERMEASURE FEASIBILITY

3.1 The Objectivity of Computer Countermeasures

(1) The nature of military countermeasures is determined by the two hostile sides necessarily obeying the dialectical law of "annihilating the enemy and preserving oneself". Due to the fact that computers have already become key equipment in C3I systems, they are the principal material foundation for the combat power of modern military forces. In conjunction with this, they have already occupied the leading position in modern military scientific and technical countermeasures. As far as computer countermeasures aimed at attacking enemy computer equipment, systems, and networks are concerned, it is possible to raise to a

maximum extent the effectiveness to cost ratios associated with military countermeasures. It is also possible to make the combat power multiplier coefficients associated with modern forces increase in accordance with the laws of exponent indices. /57

(2) The essential characterisitics associated with computer countermeasures are the basic factors determining their production, formation, and development. In conjunction with this, to a certain degree, they reflect the essential attributes of computer countermeasures. They cannot be replaced by any other countermeasure form. They are also important conditions associated with the ability to form into systems and develop rapidly. Despite the fact that people require a historical process to fully reveal, know, and grasp their essential characteristics, their objective existence, however, cannot be erased or disregarded. In reality, within a world scope, a good number of nations have already laid stress on the carrying out of research and develop with regard to them.

(3) The theoretical foundation of computer countermeasures is the determination of the prerequisite conditions associated with the final setting up of computer countermeasure combat systems (outside China, there are similar "computer warfare weapon" ideas). Computer countermeasure theory involves a broad theoretical research process, possessing a certain independence, which is the course of the computer countermeasure warfare system design, demonstration, and realization process. As far as the strengthening of the study of computer countermeasures theory is concerned, it is extremely necessary with regard to creating a scientific theoretical construct and combat systems.

(4) The construction of computer countermeasure combat systems is an objective historical process. Blind optimism is not an option. Waiting on precedent is also not a possible choice. Computer countermeasures are only remaining for a time on the level of integrated knowledge and theoretical research. It is very difficult to create computer countermeasure capabilities with all possible speed.

3.2 The Reality of Computer Countermeasures

We should then--from the reality of computer countermeasures--adequately recognize the possibility of being subjected to the threat of computer countermeasures during China's future wars to repel invasion and aggressively explore the corresponding policies we should adopt.

In the area of computer countermeasure reconnaissance, "at the beginning of March 1983, west Germany's counterespionage agency--the West German Constitutional Defense Agency--broke up a KGB spy network of the former Soviet Union stealing secrets through computers." It is said that the primary reconnaissance objectives of this net were such agencies as the U.S. Los Alamos nuclear weapons and nuclear energy research institute, the computers of the U.S. "Star Wars" research centers, the general data bases of the U.S. Department of Defense, the Geneva European nuclear energy research center, the European space research agency, the west German Heidelberg research agency, the French Tangmuxun (phonetic) industrial company, the U.S. national space agency, as well as the military agencies of U.S Forces, Germany, and so on. Of course, in the area of stealing secrets with the use of computers, the U.S. has also frequently had a hand. The U.S. weekly publication "Time" quoted a U.S. government personage as saying, "U.S. spy agencies have successfully broken into the computer systems of such countries as the (former) Soviet Union." Giving even more food for thought is a student in the former west Germany in 1988 taking his personal computer and--within two years--collecting from a network of 30 U.S. military computers large amounts national defense classified information. The information involved the "star wars project", North American Air Defense Command, nuclear weapons, as well as communications satellites, and so on. The facts above clearly show that computer countermeasure reconnaissance exists as an objective reality.

The attacks of computer countermeasure jamming are even more intense than computer countermeasure reconnaissance. Computer virus countermeasures (CVCM) have successfully attacked the largest, most important U.S. national defense and military computer network, Interet. The U.S. is profoundly threatened by computer virus jamming. It is also just in the midst of aggressively deploying developments of computer viruses for military use. Before the outbreak of the Gulf War, U.S. special operations personnel secretly used a set of micro chips carrying computer viruses supplied by the U.S. National Security Agency to substitute for the originally supplied chips in large scale computer systems associated with Iraqi control and coordination of most air defense artillery units. In an exercise carried out in November 1989, Australia also made use of computer viruses to carry out attack countermeasures training. It is said that both were successful. For just this reason, the U.S. Army has already formally announced plans to develop "super computer viruses" (computer viruses with stronger effects than ordinary viruses, and used for military purposes) in order to prepare--in time of war--to destroy enemy computer systems and networks, and, in conjunction with that, has invited bids to carry out exploratory research. The U.S. Advanced Research Planning Agency is just in the midst of developing for use wireless transmission means to implement computer virus attacks associated with "computer warfare weapons" systems in order to succeed in attempts to input from a long distance computer viruses into enemy aircraft, tanks, submarines, as well as other weapons systems and C3I systems, and, at critical moments, force the paralysis of enemy computer equipment, systems, and networks, destroying or degrading their effectiveness. Computer countermeasures destruction as well as computer countermeasure antireconnaissance, antijamming, antidestruction, and so on, have also become key subjects associated with modern electronic defense technologies. In summary, computer countermeasures exist as an objective reality.

3.3 COMPUTER COUNTERMEASURES FEASIBILITY

3.3.1 Seen with a view to the weak points inherent in computer systems themselves, computer countermeasures have the basic conditions for implementation.

(1) Environmental Factors. Computer systems have relatively high requirements with regard to environmental conditions. At the present time, there exist environmental factors which threaten normal computer system operations--in particular, field combat conditions--where the environment computers depend on is even worse. When offensive computer countermeasures are carried out, it is then possible to expand the influences of bad environment on enemy computer equipment, systems, and networks. During defensive computer countermeasures, stress should be laid on restraining the effects of bad environment on computer operations.

(2) Electromagnetic Leakage. Due to information inside computers, it is possible to generate leakage through electromagnetic waves thereby producing severe security breaches. This type of electromagnetic leakage--to a certain extent--supplies a medium for computer countermeasure reconnaissance. Moreover, it also increases the difficulty of computer countermeasure antireconnaissance. The reason lies in it not being possible to put an end to electromagnetic leakage in a good number of cases.

(3) Software Problems. Software development often caters to hardware development. Operating system design is often weighted toward increasing information processing capabilities and efficiency, and, as a result, in the area of designing system security defenses, one has the appearance of a good number of problems. Because of this, to carry out offensive computer countermeasures in the area of software alone there are a number of useablity conditions.

(4) Infiltration. Computer systems and networks use mutual connectivity as a special feature and take the common enjoyment of resources as their foundation. At a certain level, this supplies infiltration routes and advantageous conditions for

carrying out offensive computer countermeasures--in particular, unauthorized visits and illegal intrusions.

3.3.2 Seen from the viewpoint of the development of military system and computer network technologies, computer countermeasures have the basic conditions for implementation.

On the one hand, the level of dependence on computers of both antagonistic military sides follows along with increases in the degree of modernization and ceaselessly grows stronger. On the other hand, a synthesis of computer network technology as well as computer and commmunications technologies is the great trend in the development of military systems, posing problems which are difficult to overcome.

(1) Computer standardization--opting for the use of standardized software design--will set up standardized computer structures and program commands, creating mutually compatible series of equipment--for instance, PC series are just like this. In this way, it is also easy for them to be attacked by computer virus jamming. As far as opting for the use of standardized software designs is concerned, it it is possible, in the area of operating systems and applied software, to possess good compatibility. Opting for the use of standardized information formats, it is possible to improve the timeliness of data communications. Opting for the use of standardized data links is nothing else than making use of standardized output and transmission regulations as well as standardized modulation forms. This is capable of making systems and networks even more enormous. Development trends in standardization have their "positive and negative effects".

(2) Conversion to Networks in Communications. On a foundation of distributed type digital processing and programable built-in type computer development, a networked communications technology has been produced. Networked communications causes communications technology to give rise to a great revolution. According to predictions, in the communications of future battlefields, the amount of networked data communications activity will account for 40% of the total amount of communications. Modernized communications associated with distributed type digital processing and contacts supply even more modern media for the carrying out of computer countermeasure reconnaissance and jamming. The contagion of computer viruses in networked communications is capable of causing communications data flow variations. In conjunction with this, it prevents their arriving at preset terminals, and is also capable of making computer network effectiveness go down.

Computer countermeasures are capable of cleverly making use of the basic conditions of standardized computers and networked communications to realize the combat objectives of computer countermeasures.

3.3.3 Seen from the viewpoint of applying computer countermeasures technology, combat applications of computer countermeasures are just unfolding.

(1) In ten months from 1986-1987, the U.S. experimented with letting people carry out attacks on the Milnet (approximately 450 computers) within the Defense Data Network (DDN, approximately 30 thousand computers). Results showed 49% (approximately 220 instances) of successful connections. In the period of the Gulf War, a 10 year old Dutch youth called Haka (phonetic) made use of commercial computer networks and successfully connected going through the computers of a certain university and a certain computer system of the U.S. Defense Department. In conjunction with this, a portion of the information associated with U.S. personnel, equipment, and weapons systems was leaked to the outside world. At the same time, alterations were carried out on a part of the information, terrifying the U.S. military very much for a time. As a result, seen from the angle of technology and tactics, connecting with (querying) enemy computer equipment, systems, and networks is not hopeless.

(2) Theoretical reserach associated with relevent military computer virus mechanisms, design, control, and utilization has already seen breakthroughs on the foundation of currently existing computer virus research. On the basis of data introduced, a completely proficient programmer grasping computer virus mechanisms, can, within two weeks, compose a new computer virus. The U.S. "Signal" magazine reported: "There are people who doubt the feasibility of 'computer warfare' weapons. Specialists unanimously recognize that, in technological terms, there is no problem at all. All it requires is a certain amount of time and that is it." At the present time--besides the U.S--Japan's Toshiba Co. is also in the process of developing "computer warfare weapons". /59

(3) The problems of safeguarding and protecting computer systems and networks receive more serious attention with every passing day. Early on, various nations of the world extensively developed research associated with computer information system security characteristics. Going through over 20 years of effort, the U.S., in the middle 1980's, entered a period of maturity in the construction of secure computers. Only in 1985 did China begin to pay serious attention to research associated with technologies defending against electromagnetic leakage (such as Tempest). In theoretical and technological terms associated with defending against computer virus jamming, there is also a definite foundation.

3.3.4 Seen from the view point of ways to implement computer virus jamming, computer countermeasures are feasible. However, it is still necessary to overcome a number of technological difficulties.

(1) With regard to the enemy using wireless communications to connect together computer networks, it is possible, through enemy wireless communication systems, to take viruses and input them into computer systems they connect. For example, enemy intelligence collection, processing, and distribution systems, are, in reality, combinations of computers and communications systems. If one takes computer viruses and transforms them into virus code data streams and then takes the radiations through wireless transmitters at frequency points or frequency bands associated with the cut off of enemy reception--after waiting for enemy wireless systems to cut off system reception--virus flow data streams will then be capable of entering into enemy information systems. In fact, the operations (technologies) associated with turning virus programs into data streams are certainly not difficult to realize. The difficulty only lies in how virus data streams go through computer system inspection ports. At the present time, further research is needed on such key technologies as computer virus mechanisms, virus programs and communications encoding signal transformation technologies, going through quarantine connections, and so on, in order to facilitate the assisting of wireless communications inputing computer viruses to implement computer countermeasure attack actions.

(2) With regard to enemy computer networks linked together using wire channels, it is possible, through such methods as "line connection", "opening", and so on, to take computer virus code data streams and input them into enemy computer equipment, systems, and networks. At the present time, a good number of computer viruses which are already widely popular on an international scale are mostly transmited through wire channels as well as contact channels. In war time, it is possible to dispatch special action teams using specialized equipment to carry out "specified operations" on enemy wire communication channels--taking computer virus code data streams possessing directed natures and inputing them into enemy computer systems and networks. This is undoubtedly feasible.

(3) Carry out "preprocessing" on enemy computer equipment and systems. At the present time, technologies or trends have already appeared to make computer viruses "solidify" in computer equipment and systems. In reality, this is nothing else than taking computer viruses possessing specific functions and manufacturing them inside the computer software equipment. Once conditions are satisfied, the viruses will propogate, producing or manifesting the corresponding attacking power.

The brutality of military countermeasures is spuring on both hostile sides to unceasingly take possible things and turn them into realities, to take disadvantageous conditions and turn them into adantageous conditions for their own sides. Computer countermeasures are like this, too. As long as there is a possibility, "cutting edge" research and development must then be carried out.

4 A FEW SUGGESTIONS

(1) Drawing Up Computer Countermeasure Development Strategies

Beginning in the 1990's, situations where defensive computer countermeasure crises as well as opportunities and challenges associated with the development of offensive computer countermeasures exist side by side have already become a kind of irreversible trend. We should pay serious attention to the threats posed to computers, grab onto advantageous times to put computer countermeasures into initial development periods, as well as setting out early strategies for computer countermeasure development possessing the special features associated with friendly forces. Computer countermeasure development strategies are general plans for the construction of relevent computer countermeasures. They can include such contents as computer countermeasure development strategy guidance, strategic measures, and so on. They can play an active promoting role with regard to computer countermeasure development.

(2) Firmly Grasping Such Operations as Technology Management as Well as Standardization and Systemization in Computer Countermeasure Construction

The fundamental theory and applied technology of computer countermeasures are still in the early stage of development. With regard to a good number of technologies, it is necessary to expend even greater strength on research. With regard to the process of research and the fruits of technology, special attention should be paid to scientific management. In respect of the technological results in such areas as the development and application of relevent computer viruses, management and control must be under conditions of absolute secrecy. Of course, serious attention must also be paid to the construction of systematized, standardized theory and technology, to fundamentally put a stop to the appearance of confused situations associated with computer countermeasure construction.

(3) Clarify Computer Countermeasure Development Powers and

Responsibilities and Construct Smooth Relationships

As far as the initial period of computer countermeasure development is concerned, there are a good number of concrete operations which must be performed. A lack of clearly specified responsibilities and powers will be bound to create "delaying effects" in development. One is the policy making and implemememtation responsibilities between leading agencies and implementing units. The second is the coordination and subordination relationships between scientific research institutions and industrial departments as well as links in the production chain. The third is the relationships of the leading and the led between the military and localities. The military must, in a timely manner, notify relevent research institutes and production plants of the requirements associated with research--on the basis of the overall needs of the military--and of development plans which will suit future computer countermeasure requirements to supply production prototypes which have real combat capabilities, and, in conjunction with this, capable of guiding the production of manufacturing plants. Fourth is the relative importance and urgency of academic research and the tackling of key technological tasks. In summary, as far as the construction of computer countermeasure combat systems is concerned, there should be a clear division of labor and close coordination beginning now. Otherwise, it will not then be possible to have vigorous development momentum.

(4) Set About the Construction of Computer Countermeasure Experimental Simulation Systems

Up to the present time, a good number of conclusive theories have all been obtained on the foundation of qualitative analysis and possess certain limitations. It must be recognized that to realize computer countermeasure development strategies is a historical process. It must also be recognized that the obtaining of scientific conclusions is a product of the mutual combining of qualitative and quantitative analysis. As a result, the setting up of experimental computer countermeasure simulation systems is even more important and pressing. For instance, during the carrying out of feasibility analysis of using wireless means to input computer viruses, it is necessary to have large amounts of empirical conclusions to act as the basis of the analysis.

(5) Strengthen Advance Research Work Associated with Computer Countermeasures and Push Forward the Construction Pace on a Unified Computer Countermeasure and C3I System

As far as the entire process of information detection, information transmission, and the carrying out of command, control and policy making is concerned, in reality, it is a process which combines the effects of multiple levels, multiple means, and multiple types of situation responses. Among these, computer countermeasures will exert effects which cannot be allowed to be ignored. If it is desired, in the future, to form computer countermeasure capabilities, it is then necessary to carry out relevent advance research in order to facilitate the laying of a good foundation for later development. At the same time, it is necessary to see that computer countermeasures are systematic countermeasures of "system with system". During the process of setting up computer countermeasure combat systems, attention must be paid to the construction of their own command automation.

(6) Cultivating Talent Capable of Engaging in Computer Countermeasures Research

Computer countermeasures are a new realm of military countermeasures in the age of high technology and science. Its development speed will far, far surpass the development speed of traditional military countermeasures. If one wishes to do research and development on computer countermeasures, it is necessary to have specialized talent. Before the 1960's, most specialists beginning to be engaged in electronic countermeasures research were on the point of gradually withdrawing from the front line of scientific research. Moreover, a good number of personnel among them actually had quite a few concrete difficulties with regard to assuming the responsibility for the important work of computer countermeasure scientific research. As far as the faulting phenomena created by the Great Cultural Revolution are concerned, they also caused a rift to appear in the ranks of scientific research. As a result, it was necessary to begin cultivating from youth software research personnel capable of engaging in the computer countermeasures specialty and to cultivate scientific and technical personnel capable of engaging in computer countermeasure warfare systems development (particularly, software design and systems projects), in order to have a planned assumption of responsibilities for a portion of advance research topics. During realization, experts were gradually produced for computer countermeasure scientific research. There was also a desire to have a planned recruitment and cultivation of other specialized talent with the aim of engaging in computer countermeasures research, replenishing scientific research strength associated with computer countermeasures.

(7) Firmly Adhering to and Perfecting Research Methods

Associated with the Combined Use of Technical Experts and Military Experts

In high technology realms--wanting to correct the lack of a trend in thought with regard to electronics countermeasures--it is necessary to go the route of combining technology experts and military experts with each other, causing a computer countermeasures short cut to be built. During the process of setting up and verifying computer countermeasure combat system designs, one wants to exert the advantage in macro thought associated with military experts to cause computer countermeasure theoretical systems, technical models, and combat systems to be set up on a foundation of scientific, technological, and battlefield requirements. In the actualization phase of computer countermeasure combat system designs, one wants, in particular, to exert the technological advantage associated with technical experts to cause the construction of combat systems to have reliable technological guarantees. Any computer countermeasures research which cuts out the participation of technical or tactical experts is, in all cases, inadequately scientific research methodology.

REFERENCES

1 Computer Virus Countermeasures A New Type of EW. Defence Electronics，1989(10)。

2 李京夫译.未来战争中的新式武器——计算机战武器.军事电子，1991(4)。

3 张云秀，戎建刚.计算机对抗.航天电子对抗，1991(1)。

4 计算机信息系统的安全问题及其对策.中国计算机报，1991(49)。

5 孙宪立.计算机间谍之战.军队指挥自动化，1990(1)。

6 刘尊全.计算机病毒防范与信息对抗技术.北京：清华大学出版社，1991(5)。

7 杨劼.关于计算机对抗的研究.机电部“9204”会议论文集〔内部资料〕，1992.4.

DISTRIBUTION LIST

DISTRIBUTION DIRECT TO RECIPIENT

ORGANIZATION	MICROFICHE
B085 DIA/RTS-2FI	1
C509 BALLOC509 BALLISTIC RES LAB	1
C510 R&T LABS/AVEADCOM	1
C513 ARRADCOM	1
C535 AVRADCOM/TSARCOM	1
C539 TRASANA	1
Q592 FSTC	4
Q619 MSIC REDSTONE	1
Q008 NTIC	1
Q043 AFMIC-IS	1
E404 AEDC/DOF	1
E410 AFDTC/IN	1
E429 SD/IND	1
P005 DOE/ISA/DDI	1
1051 AFIT/LDE	1
P090 NSA/CDB	1

Microfiche Nbr: FTD95C000693
NAIC-ID(RS)T-0267-95